THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 16 Article 5

11-8-2021

DON'T BITE THE BAIT: PHISHING ATTACK FOR INTERNET BANKING (E-BANKING)

ilker Kara
Cankiri Karatekin University, karaikab@gmail.com

DON'T BITE THE BAIT: PHISHING ATTACK FOR INTERNET BANKING (E-BANKING)

Ilker Kara
Department of Medical Services and Techniques, Eldivan Medical Services Vocational School
Çankırı, Karatekin University, Turkey
karaikab@gmail.com

ABSTRACT

Phishing attacks are based on obtaining desired information from users quickly and easily with the help of misdirection, panic, curiosity, or excitement. Most phishing websites are designed on internet banking(e-banking), and the attackers can acquire financial information of misled users with the tactics and discourses they develop. Despite the increase of prevention techniques against phishing attacks day by day, an effective solution could not be found for this issue due to the human factor. Because of this reason, attackers' attack techniques and strategies from actual phishing attacks are essential to study and analyze. This study focused on the detection and analysis of a real e-banking phishing attack using the phishing website. Analysis results show that the attacker's information is traceable.

Keywords: Mobile phishing, Phishing website, Phishing attacks analysis, e-banking phishing, Cyber security, Forensic analysis

1. INTRODUCTION

The phishing attack is an attack-type that is intended to retrieve the victim's personal information (social media username, password, bank account number, username, etc.) in the network environment. The attack concept is as old as human history. Its purpose, application varieties, and techniques have continuously developed, becoming a more complex and difficult problem to solve today. Improvements in technology and rapid increase in its usage have brought improved attack risk in attack types and techniques, and it has also increased the exposure to cybercrime. The word "phishing" itself is a combination of the words "password" and "fishing." Phishing attacks were first seen in the early 2000s.

According to Brand et al. (2010), phishing attacks have become a cyber-attack tool developed to deceive and defraud users by using fake websites, fake emails, and malware, and today it is used virtually. According to Retruster's published report, millions of people have been affected by phishing attacks, and 90% of data breaches use this method Retruster (2019).

The literature shows that phishing attack scenarios happen in three stages: attack preparation, attack method, and phishing attacks (See Fig 1). Attackers get through the exhaustive preparation phase before the attack. In the attack preparation phase, the at-

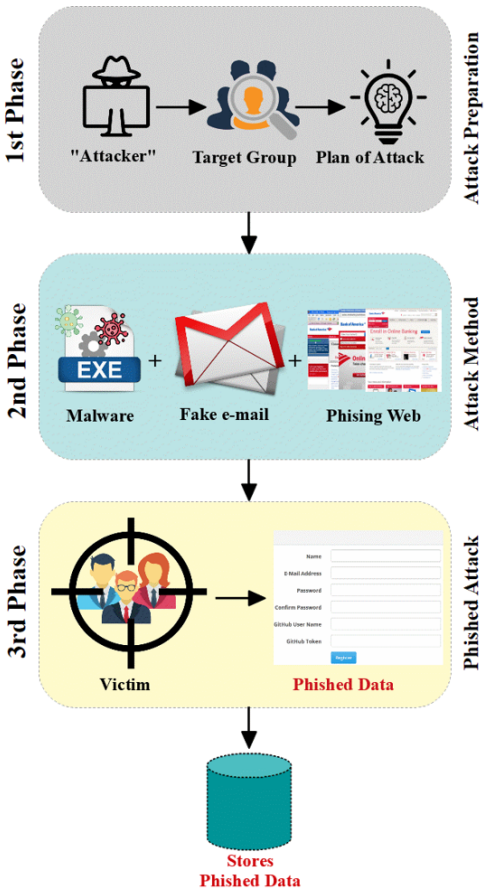

Figure 1. Commonly employed phishing attacks in the literature.

tacker determines the target group and plans an attack for that group. After choosing a target according to their motivation, they begin to gather information about the targets. They aim to increase the success rate for their phishing attack in an organized and systematized way. They collect information by exploiting people's vulnerabilities, especially social media accounts, mail addresses, family, friends, and even people unrelated to the target. Social media accounts or mail addresses are indispensable data sources. Current political or social events and their effects on the people are also used in the data collection phase.

In the attack method phase, attackers use malware attached to emails, fake web pages, etc. Web-based phishing attacks use an email containing a malicious link or web page, which at first glance appears to be from a corporate company, to reach the attacker's victims Dhanalakshmi and Chellappan (2010); Meghanathan et al. (2010). The suspicious email is aimed at obtaining important information about the victim. The discourse and tactics developed by the attackers are aimed at confusing and bringing emotions to the forefront. Digital forensics experts examine digital evidence, such as suspicious emails, to identify criminal elements Dhanalakshmi et al. (2011).

According to Das et al. (2018), reducing phishing attacks using safety tools and user-specific warnings can prevent attacks in the preparation phase. Despite these measures, the surprising variety of end-users and their roles in this process could not be understood. One of the most common methods used in phishing attacks is to reach users via email and notifications that will cause panic, curiosity, and excitement in them Jolly (2016). If the user clicks on the malware in the email attachment or the link which belongs to a fake web page, the user will be redirected to a tricky web page that looks like one of the

legitimate institutions or a bank (Basit et al., 2020).

According to Chaudhry et al. (2016), it has been pointed out that in many detected phishing attacks, especially the keylogger type malware, the email attachment is preferred by attackers to capture the user's passwords.

In the last few years, one of the most threatening phishing attacks has been an attack that aims at internet banking. The attacker aims to deceive the people they reach by clicking a fake link that enables the target person to enter their information in the relevant sections in this link. Because of this careless and rushed process, the attacker will be able to retrieve all necessary information for internet banking. The attacker designs these web pages to be difficult to distinguish from the relevant pages of the institution or organization they are imitating Chanajitt et al. (2018). When the users visit these web pages designed by the attackers to mimic e-banking pages for financial gain, they may seem almost identical to the current view of the relevant bank's page Aburrous et al. (2010); Junger et al. (2017).

At the time of the attack, the victim is performing e-banking activities, while the attacker is between the customer and the bank, and the customers use their online banking accounts Adham et al. (2013); Hertzum et al. (2004).

According to Gan et al. (2008), e-banking attacks have been arranged via a fake web page link for Malaysian Computer Emergency ResponseTeam or MyCERT. According to this report, there were 3 cases in 2000, 106 cases in 2004, and 364 cases in 2007, and it was noted that such attacks increased dramatically. After the phishing attack phase has been completed, the attacker does not achieve its purpose by obtaining the financial and personal information of the user. Later, these users' passwords, social media accounts, financial data may be used to collect money or perform financial frauds such as transferring funds and purchasing goods through electronic commerce Hertzum et al. (2004).

New methods are being developed to fight against this crime. Otrok et al. (2014), to prevent phishing attacks, a method was proposed that includes programming to invalidate access permissions in suspicious transactions; it cannot prevent attacks due to the possibility of benefiting from this method and human factors, and these attacks are still a major threat. Considering all of these, in this study, we present an approach that shows how to detect and analyze phishing attacks. For this purpose, this study mainly presents four contributions:

- This study focuses on phishing attacks against e-banking and provides an approach to how to examine the detection and analysis of these attacks.
- For this purpose, a phishing attack case for real e-banking has been selected, the attack detection and analysis have been examined, and the results have been evaluated.
- To be more precise, we evaluated the working mechanism of the phishing website designed, the processes performed, and the forensic analysis for the phishing attack.
- In the light of the obtained analysis results, we saw that the attacker was traceable and evaluated the contribution of phishing website analysis to forensic investigations.

This article is organized as follows: in section 2, we have reviewed some relevant studies. In section 3, we performed a case detection and analysis for a real e-banking phishing attack. In section 4 presents an evaluation of the approach used. Lastly, section

5 completes the work and explains possible solutions to fight against phishing attacks that might occur in the future.

2. BACKGROUND KNOWLEDGE AND RELATED WORK

In the present day, there are many studies in the field of phishing attack detection and analysis. In this section, some of these studies, especially on analysis for e-banking, have been briefly reviewed.

Wardman et al. (2014), in the study they did in 2010, presented a dataset consisting of URLs to these organizations that were targeted by phishing attacks against e-banking. The attackers mentioned that they created 88,331 URLs and various websites associated with them to organize e-banking phishing attacks against the target organizations. As a result of the study, they argued that to fight against a phishing attack, these websites designed specifically for e-banking and phishing attacks can be detected and blocked with techniques such as URL information. According to Dhamija and Tygar (2005), the attackers usually use web-based applications to organize e-banking phishing attacks to profit; in addition to that, users have emphasized that these websites are too difficult to distinguish from a real application. They stated that to prevent these attacks; the companies should use e-banking applications that minimize the risk by considering this threat.

Kshetri (2006) has analyzed the cost-benefit structure of the attackers and mentioned that the existing protection mechanisms are insufficient in detection and analysis; therefore, research to fight against this crime should be increased necessarily. In addition, they explained that the periodic analysis reports about phishing attacks raise awareness in society and will pay attention to this issue. Thus the attackers will be arrested and discouraged.

In their study, Aburrous et al. (2010) proposed an analysis model using a data set consisting of three case studies of phone phishing, website phishing, phishing website survey scenario, which they determined for e-banking phishing attacks. As a result of the study, it showed that the security systems used in the study did not show enough awareness for the users while applying the social engineering elements of the organized training programs.

According to Kirda and Kruegel (2005), if the websites used in e-banking phishing attacks can be detected with the anti-phish method and detected as soon as confidential pieces of information such as passwords have been typed in the forms on these websites, the pending transactions on these websites can be canceled before they are being used. They describe that if the form that they are filling belongs to an untrusted website and generates an alert, it would cancel the pending transaction. This approach is important to prevent the threat before it occurs by creating an e-learning model. Unfortunately, prior knowledge about the target website is required for the web-based restriction approach to be applicable. Under these circumstances, this might not always be available. More importantly, the success rate is very limited because the attackers are also aware of this approach and develop techniques to circumvent this detection.

Another similar popular approach is the URL-based detection of web pages by Teraguchi et al. (2014). This approach is based on detecting phishing attacks by evaluating the invalid or hidden URL and preventing the attack. The disadvantage of this approach is the attackers create a fake user account at the login step and hide the real URL.

Herzberg and Gbara (2004) proposed the "TrustBar" approach to avoid phishing attacks. This approach detects important logos

and other graphic content on official websites and identifies fake ones. However, this approach could not accomplish the desired effective result because the attackers use the same logos and graphic contents located on official websites on the fake websites they develop. The successes are low in this and similar approaches because the attackers develop methods to circumvent these kinds of techniques (i.e., web page or URLs such as blacklist, fraud detection, anti-phishing toolbars, or spam filters).

Pan et al. (2006) proposed to first analyze the real identities of websites to detect website-based phishing attacks. For this purpose, this includes the title, description, pictures and videos, copyright, etc., on the website. They assumed that features such as phishing might be changed by the attacker while preparing phishing websites. As a result of the study, it was seen that the proposed method was unsuccessful at a rate of 29%. In another study, Yi et al. (2018) proposed a method for detecting phishing websites designed to steal victims' usernames, identity information, and credit card information. The study aims to detect the IP numbers and URL addresses of suspicious websites using deep convolutional neural networks (CNN) method and to block these websites. In the study, real data from the ISP (Internet service provider) within 24 hours was used as the data set. As a result of the study, it was seen that the proposed method had a success rate of 90%.

3. MATERIALS AND METHODS

In this section, we introduce the Workstation and analysis tools used in the analysis. Then, a real case of e-banking phishing attacks is described.

3.1 Case Study Dataset

The importance of choosing a well-chosen and correct case is vital for case study-focused studies and is a well-known fact. If e-banking phishing attacks are reviewed, there are a limited number of data sets available, such as Aburrous et al. (2010) and Wardman et al. (2011). In addition, the fact that the case study to be used in the analysis should be a real attack case is critical in determining the detection and analysis approaches. Therefore, the available datasets were not suitable for our research.

We collaborated with an information security company in Turkey to reach such an appropriate case study. The mentioned company has a dedicated team and system to collect many phishing attack software samples (e-banking). They shared the real example of e-banking phishing attacks with us. Please note that the selected example is purposed especially for e-banking phishing attacks.

3.2 Preparation of Analysis Environment

All analyses were performed on a Dell Precision T3630 brand Workstation with Xeon E-2124/8GB/1TB HDD Quadro P620 running Windows 10 Pro software. The victim has taken a copy of the cell phone in digital image E01 format using UFED-Cellebrite instead of doing a live investigation on the mobile phone that they were using. Analyzing the live system may involve some risks. A possible risk is not compromising data integrity so that the analyses are reproducible for different people or different analysis environments. For this purpose, all analysis has been performed via digital copy. The digital image does not change the original data. It ensures data integrity by verifying the original mobile phone information system and the digital copy obtained with the help of MD5 (Message-Digest the algorithm, MD5)

or SHA-1 (Secure Hashing Algorithm, Sha), Sha-256 hash values (Table 1). Analysis has been performed in the virtual machine in the Workstation, using Cellebrite Physical Analyzer 7.22 tools. Since the selected example is a real cyberattack and forensic case, some information has been presented in the study by hiding.

3.3 Case Study

The victim wishes to perform online banking transactions on the web page of Is Bank, and, for this purpose, he is searching for the word "Isbank" in www.google.com.tr on his mobile phone and clicking on the link that he thinks belongs to the e-banking system of the relevant bank. While he was logged in, he received an informative message from his account that $1200 was transferred without his knowledge. When he checked this suspicious transaction checked in his account, he saw that the transaction indeed took place without his knowledge. For this reason, he applied for a judicial application to investigate the issue.

For this purpose, images of the victim's mobile phone were taken using the UFED-Cellebrite program, and investigations were started with the UFED-Cellebrite Analyzer 7.22 program on the Workstation. The internet records of the victim's statements of 21.06.2020, which is the date of suspicious transactions, were examined (see Figure 2).

As shown in Figure 2, a search was done with the word "ISBANK" on the `www.google.com.tr` search engine on the day of the suspicious event. While the victim was trying to make an e-banking transaction, it was detected that the domain name was likened to the official bank address at first glance and entered the domain `http://isbanh.com`. This domain name was specially designed for the e-banking phishing attack, and it was concluded that the victim's e-banking information had been collected. The focus of the investigation was to identify the suspicious web addresses of victims from the internet records (Figure 3). The screenshot of the website was given in Figure 3, where you can look at the access link of the suspicious website and the area where the bank customers enter their personal information.

HTTrack Website Copier is a website copy tool that allows you to download the entire website to the computer and allows the downloaded website to be used offline. In order to examine the suspicious website content, the suspicious website `http://isbanh.com` was downloaded to the Workstation using HTTrack Website Copier 3.49-2 program, and the contents of the suspect site were reached (Figure 4). The folders on the website (1), the index operator that allows viewing the offline pages of the internet- (2) and log files in which the information of the visitors who enter the field on the website is kept- (3) are shown in Figure 4.

By running the website's index operator, the "view page source" examination of the site was made (Figure 5).

From the view page source examination of the suspect `http://isbanh.com` website, it was seen that the website was prepared with word press, and a "MetaWeblog" was created to write the entries that entered the website using web services. The log file seen in the website content was shown (Figure 6). Figure 6 shows the suspicious `http://isbanh.com` website log records: the victim whose personal information was obtained by the phishing attack (1) and the other victim whose personal information was obtained by the phishing attack (2). After the forensic examination of the suspect website's content, it concentrated on accessing the information of the attacker. Identifying the IP number of the suspicious website is one of the most widely used methods to reach the attacker in forensic investigations. It is the detection of the suspicious IP number and then the

Product Name	Samsung Galaxy A71
Product ID	326153051670XXX
Operating System	Android
Operating System Version	Android 10.0
Install Date	10.04.2016 - 10:47:35 UTC
Shutdown Time	17.12.2020 - 07:14:15 UTC
Description	Physical Disk, 132.443 Sectors 13,2 GB
Total Size	72.332.3346 Bytes (13,2 GB)
Total Sectors	132.443
Acquisition MD5	4gfabbbest32eaa456a727e0c3as67231
VerificationMD5	4gfabbbest32eaa456a727e0c3as67231
AcquisitionSHA1	ca34ca676c2ae562f06ca566f62990acd34a4b
VerificationSHA1	ca34ca676c2ae562f06ca566f62990acd34a4b

Table 1. Device information.

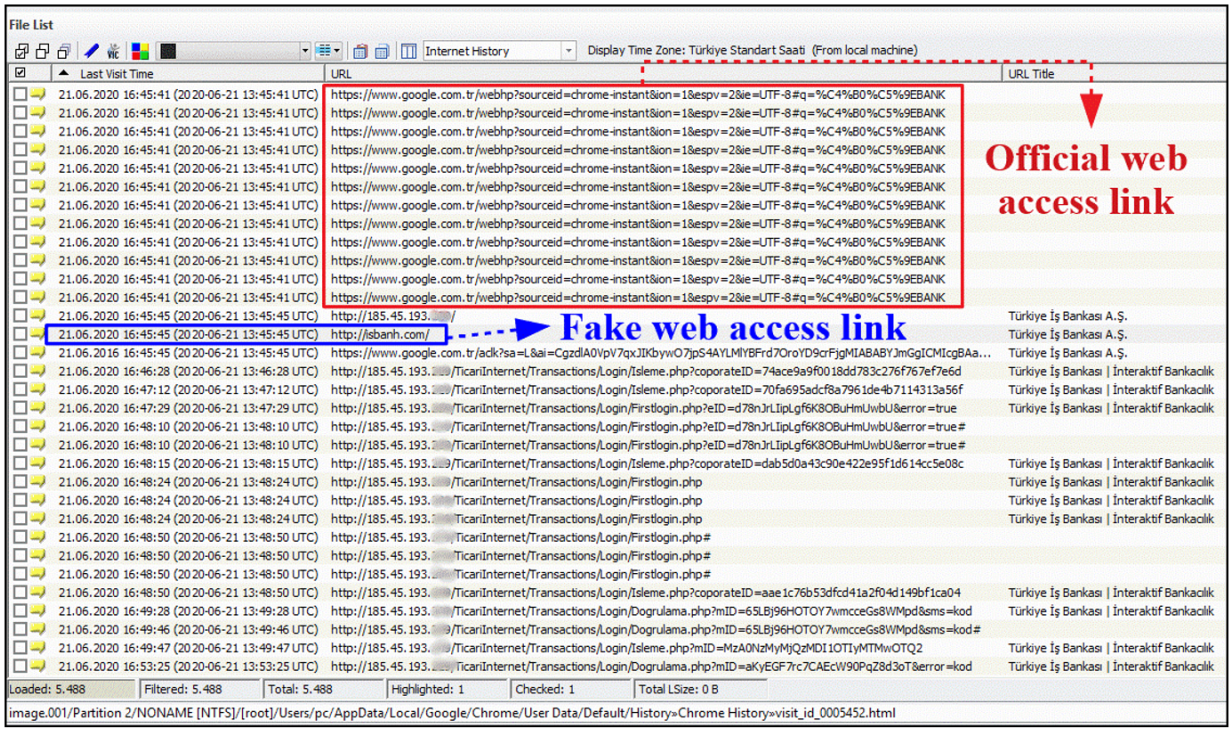

Figure 2. Screenshot of the query of suspect IP address.

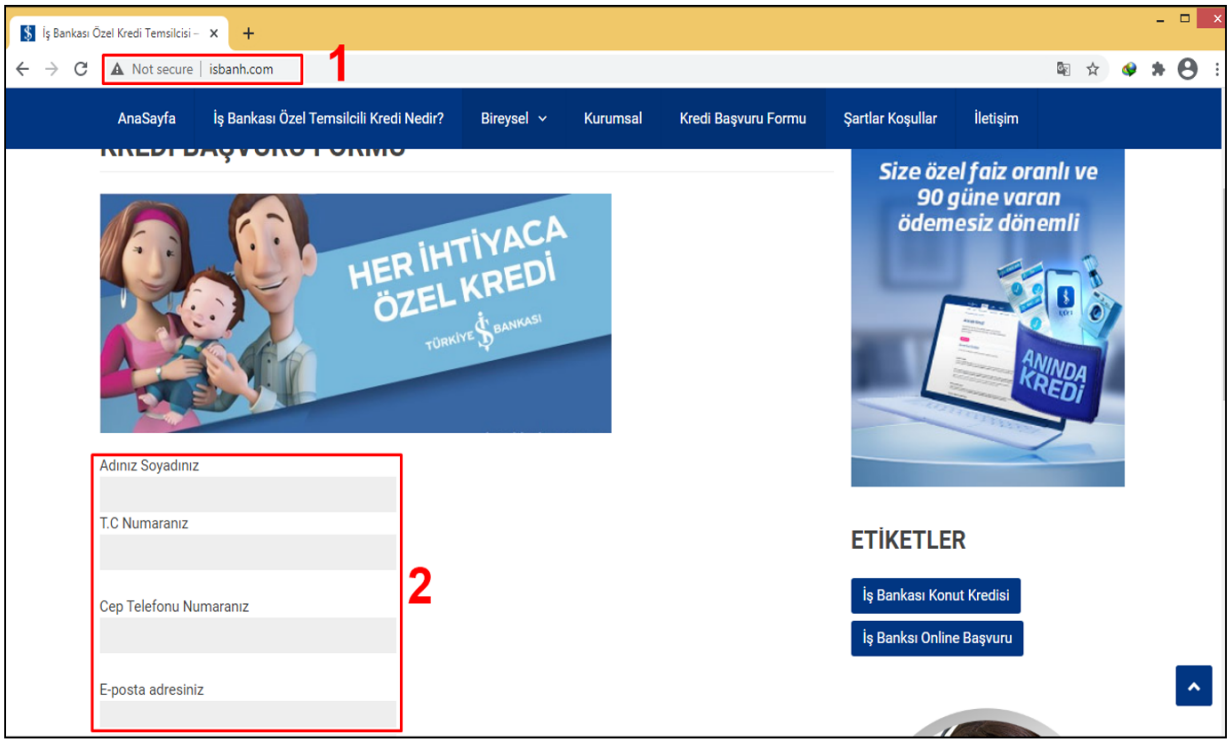

Figure 3. Screenshot of the website's view suspect `http://isbanh.com`.

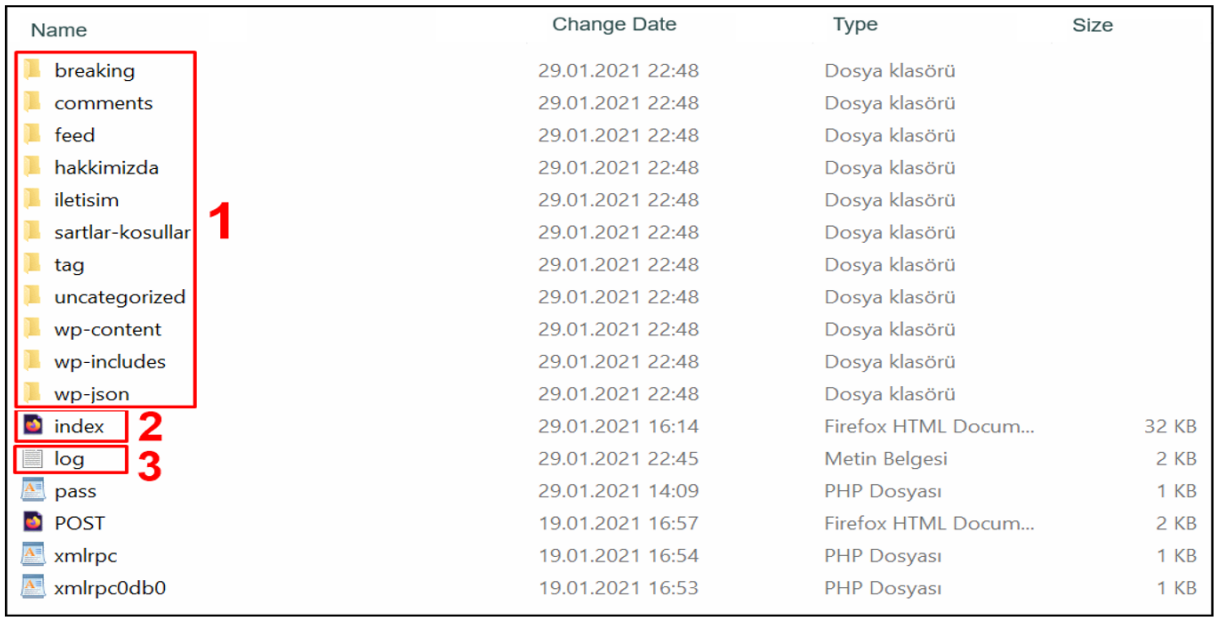

Figure 4. Content of the suspected http://isbanh.com website with the HTTrack Website Copier program.

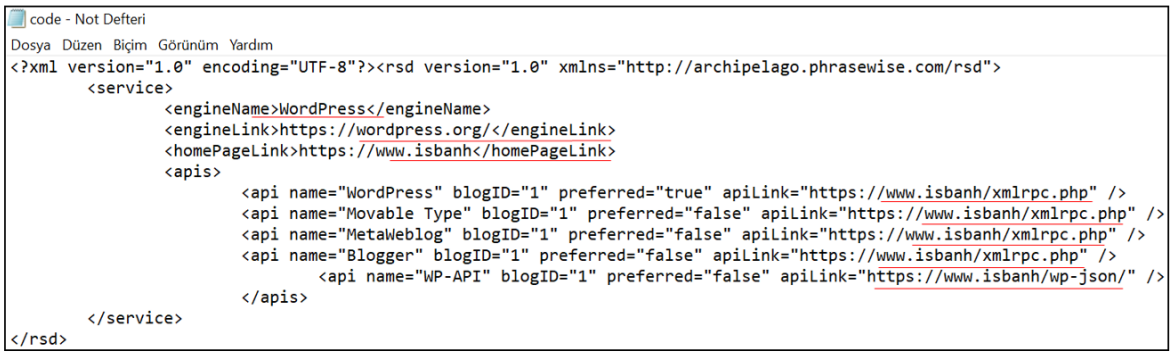

Figure 5. Screenshot of the website's view suspect `http://isbanh.com`.

determination of the internet subscriber to which the IP number is assigned. If this information is available, it can often provide the opportunity to track the attacker.

As a result of the analysis, the domain name of `http://isbanh.com` was seen by accessing with the IP address "185.45.193.XXX" (See Figure 7). After determining the type of attack, investigations focused on the attacker-based information thought to be belonging to the attacker in order to reach the attacker. For this purpose, the domain name "isbanh.com" and IP address were inquired from the IP, www.domaintools.com address (See Figure 3). As a result of the query, it was seen that the information thought to belong to the attacker was accessible.

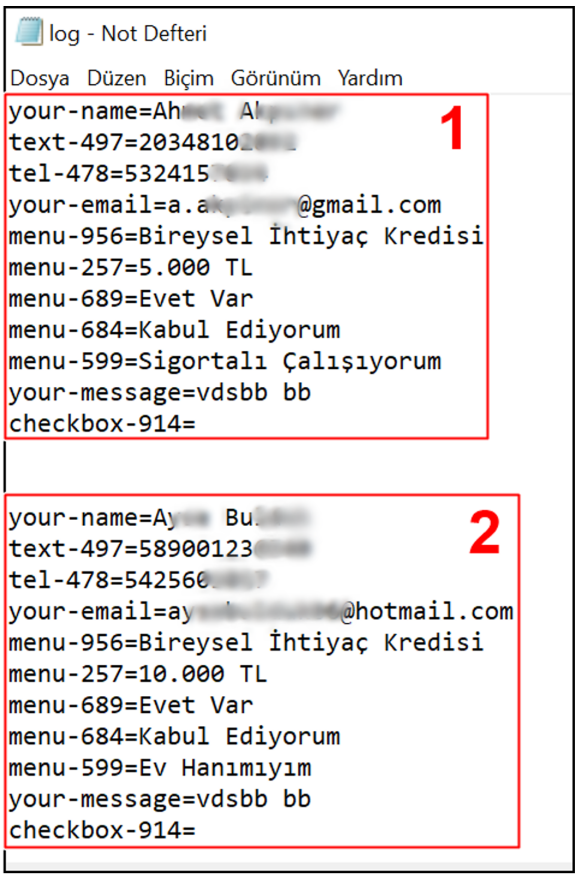

Figure 6. Screenshot of the website's view page source.

4. DISCUSSION

The proposed scheme, similar to Riadi et al. (2013), is mainly based on detecting and analyzing phishing attacks with the help of forensic analysis tools. The content of phishing attacks in this study is identified as a real case study. The examined example of e-banking phishing attacks is identified as a popular type of cyberattack designed to have financial gain by attackers, which has been frequently seen recently. Analyses offer two important advantages, such as (1) the

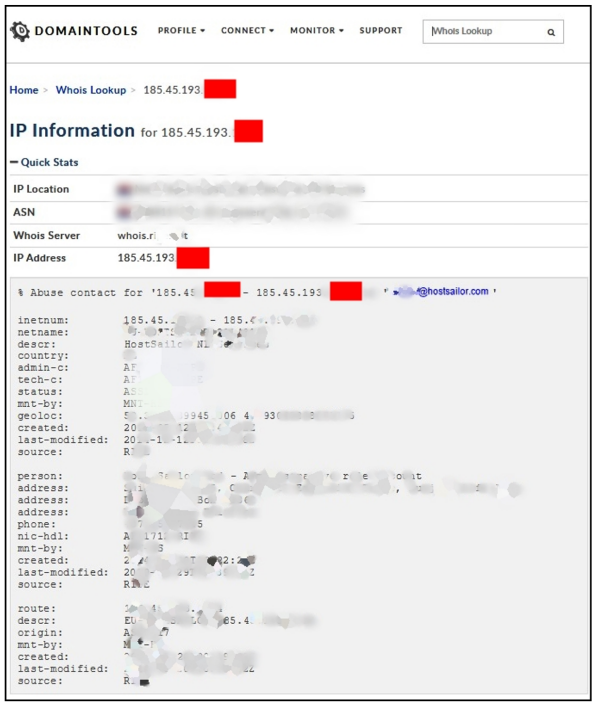

Figure 7. Screenshot of "`https://whois.domaintools.com`" query of detected suspect IP number.

e-banking phishing attack detection and analysis, and (2) even the attack method used, to be able to trace the information that is thought to belong to the attacker. On the other hand, e-banking phishing attacks analysis has some difficulties. First of all, although each attack is similar to the others, it can be designed differently, and the analysis approach may differ depending on the case. For this reason, many security professionals are constantly reviewing the latest attacks or prefer to do open-source research on studies in this area to deal with this threat. To overcome this problem, some approaches have been proposed, such as customizing a web page as proposed by Emigh (2005), in which bank and trust companies can send a unique personalized message to their customers or upload a photo of the user. They also argued that the use of personalized web pages could not imitate the attackers' deceptive emails or web pages. These kinds of attempts against an e-banking phishing attack are hopeful of fighting against that crime.

Another study, which is closer to a part of our study, Al Mutawa et al., conducted a forensic analysis of phishing websites on smartphones using forensic analysis tools (UFED-Cellebrite, Wireshark, etc.) Al Mutawa et al. (2012). Although the proposed method in the study is applicable for similar forensic cases, they emphasized the necessity of performing analyses with different models and brands of smart mobile phones. This study analyzed and detected real e-banking phishing attack examples. It was seen that the information of the attacker was accessible from the analysis results. Moreover, the analysis of the real sample selected in the study showed that the content analysis of the phishing website, determination of the attack strategy, and information about the attacker could be reached. This result shows that the approach used in the study can be a suitable method that can be used, especially in the analysis of phishing web attacks. We believe this approach needs to be repeated with more current examples to support this approach strongly. Another remarkable topic is the potential of deep learning methods that we can utilize. As we highlighted in previous chapters, we believe that achieving high success in e-banking phishing attack prevention can contribute to the problem area.

5. CONCLUSION

In this study, we conducted a study involving a real case study for e-banking phishing attack detection and analysis. Furthermore, the analysis showed that the information of the attacker was traceable. The approach used in the study shows that it is an appropriate method that can be used in e-banking phishing attack detection and analysis. We plan to investigate the analysis platform us-

ing deep learning methods in e-banking phishing attack detection and analysis in a future study. We believe that deep convolutional neural networks (CNN) methods can contribute to large-scale phishing attack detection and analysis in the problem area. The rationale behind this argument stems from our observations of phishing attacks and the focus of attention mechanisms in modern CNN's for where to look in phishing attacks to discover the most distinctive regions automatically.

REFERENCES

[1] Aburrous, M., Hossain, M. A., Dahal, K., Thabtah, F. Experimental case studies for investigating e-banking phishing techniques and attack strategies, Cognitive Computation, 2010; 2(3), 242-253.

[2] Al Mutawa, N., Baggili, I., Marrington, A. (2012). Forensic analysis of social networking applications on mobile devices. Digital investigation, 9, 24-33.

[3] Adham, M., Azodi, A., Desmedt, Y., Karaolis, I. How to attack two-factor authentication internet banking. In International Conference on Financial Cryptography and Data Security, 2013; 322-328.

[4] Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., Kifayat, K.. A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommunication Systems. 2020; 1-16.

[5] Brand, M., Valli, C., Woodward, A. (2010). Malware forensics: Discovery of the intent of deception. Journal of Digital Forensics, Security and Law, 5(4), 1-11.

[6] Chaudhry, JA., Chaudhry, SA., Rittenhouse, RG. Phishing attacks and defenses. International Journal of Security and Its Applications, 2016; 10(1), 247-256.

[7] Chanajitt, R., Viriyasitavat, W., Choo, K. K. R. Forensic analysis and security assessment of Android m-banking apps. Australian Journal of Forensic Sciences, (2018). 50(1), 3-19.

[8] Chowdhury, T., Vidalis, S. (2012, September). Collecting evidence from large-scale heterogeneous virtual computing infrastructures using Website Capture. In 2012 Third International Conference on Emerging Intelligent Data and Web Technologies IEEE,211-217.

[9] Das, S., Kim, D., Kelley, T., Camp, L. J. (2018). Grifting in the Digital Age, PrivacyCon.

[10] Dhamija, R., Tygar, JD. The battle against phishing: Dynamic security skins. In Proceedings of the 2005 symposium on Usable privacy and security, 2005;77-88.

[11] Dhanalakshmi, R., Chellappan, C. (2010, July). Detection and recognition of file masquerading for email and data security. In International Conference on Network Security and Applications Springer, Berlin, Heidelberg, 253-262.

[12] Dhanalakshmi, R., Chellappan, C., Liu, Q. (2011). Mitigating Email Threats-A Web Content Based Application. In Proceedings of International MultiConference of Engineers and Computer Scientists, 2011; 1.

[13] Emigh A. Online identity theft: phishing technology, chokepoints, and countermeasures. ITTC Report on Online Identity Theft Technology and Counter measures, 2005; 1- 58.

[14] Gan, GGG., Ling, TN., Yih, GC., Eze, UC. Phishing: a growing challenge for Internet banking providers in Malaysia. Communications of the IBIMA. 2008;5, 133- 142.

[15] Hertzum, M., Jørgensen, N., Nørgaard, M. Usable security and e-banking: Ease of use vis-a-vis security. Australasian Journal of Information Systems, 2004;11(2).

[16] Herzberg, A., Gbara, A. Trustbar: Protecting (even naive) web users from spoofing and phishing attacks. Cryptology ePrint Archive, Report 2004/155. Retrieved from http://eprint.iacr.org/2004/155. (2004).

[17] Junger M, Montoya L, Overink FJ. Priming and warnings are not effective to prevent social engineering attacks. Computers in human behavior, 2017; 66, 75-87.

[18] Jolly, V., The influence of internet banking on the efficiency and cost savings for banks' customers. International Journal of Social Sciences and Management, 2016; 3.3: 163-170.

[19] Kshetri, N. The simple economics of cybercrimes. IEEE Security Privacy, 2006; 4(1), 33-39.

[20] Kirda, E., Kruegel, C. Protecting users against phishing attacks with antiphish. In 29th Annual International Computer Software and Applications Conference (COMPSAC'05), 2005;517-524.

[21] Kruegel C, Kirda E. Protecting users against phishing attacks. The Computer Journal, 2005; 1- 8.

[22] Meghanathan, N., Boumerdassi, S., Chaki, N., Nagamalai, D. (Eds.). (2010). Recent Trends in Network Security and Applications: Third International Conference, CNSA 2010, Springer

[23] Chennai, India, July 23-25, 2010; 89.

[24] Pan, Y., Ding, X. (2006, December). Anomaly based web phishing page detection. In 2006 22nd Annual Computer Security Applications Conference (ACSAC'06) IEEE, 381-392.

[25] Retruster Website. (2019), 2019 Phishing Statistics and Fraud Statistics, Retrieved from https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html.

[26] Teraguchi, N. C. R. L. Y., Mitchell, J. C. (2004). Client-side defense against web-based identity theft. Computer Science Department, Stanford University. Available: http://crypto. Stanford. edu/SpoofGuard/webspoof. pdf.

[27] Otrok, H., Mizouni, R., Bentahar, J. Mobile phishing attack for Android platform. In 2014 10th International Conference on Innovations in Information Technology. 2014;18-23.

[28] Riadi, I., Istiyanto, J. E., Ashari, A. Log analysis techniques using clustering in network forensics. arXiv preprint arXiv:1307.0072. (2013).

[29] Yi, P., Guan, Y., Zou, F., Yao, Y., Wang, W., Zhu, T. (2018). Web phishing detection using a deep learning framework. Wireless Communications and Mobile Computing, 2018.

[30] Wardman, B., Stallings, T., Warner, G., Skjellum, A. High-performance content-based phishing attack detection. In 2011 eCrime Researchers Summit, 2011;1-9.

